Password Creation Rules

Category: Security & Logging In

DRAFT

This article is being reviewed for completeness and technical accuracy.

Your password is vulnerable to attack since it can be guessed. Follow the rules below when creating your NAS passwords:

1. Never use a password at NAS that has ever been used by you anywhere else, and never use the password that you create for NAS anywhere else, ever.

2. A password must contain a minimum of 8 characters. It must contain one character each from at least three of the following character sets: uppercase letters, lowercase letters, numbers, and special characters.

3. Use non-trivial passwords; examples of "trivial" passwords that you may not use include but are not limited to:

   ♦ your user ID
   ♦ a dictionary word of any language or a dictionary word with numbers appended or prepended to it
   ♦ a password either wholly or predominately composed of the following: user ID, owner name, birthdate, Social Security Number, family member or pet's name, name spelled backwards, or other personal information
   ♦ a contractor name
   ♦ a division or branch name
   ♦ repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
   ♦ the name of any automobile or sport team
   ♦ the name of any vendor product or nickname for a product

4. A new password can not be any one of your last 24 passwords.

5. Once you are successful in changing a password, you have to wait at least 7 days to change it again.

6. Passwords must be changed every 90 days.

Never share your password with anyone. For more information, read <u>Account Policies</u> and the <u>Acceptable Use Statement</u>.

Article ID: 270
Last updated: 03 Jun, 2011
The HEC Environment -> Security & Logging In -> Password Creation Rules
http://www.nas.nasa.gov/hecc/support/kb/entry/270/?ajax=1